Our ref 1292057

Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6795

Nicholas.Jajko@kennedyslaw.com

November 19, 2025

Via Online Submission

Office of the Attorney General
Consumer Affairs Response Team
2115 State Capitol, Lincoln, NE 68509

Re: **City of Michigan City, IN – Notice of Data Event**

Dear Sir or Madam:

We represent the City of Michigan City ("the City"), a municipality in Indiana. We write in accordance with the Nebraska breach of personal information notification statute, NEB. REV. STAT. § 87-803 (2016), to report a data event impacting the personal information of one (1) resident of Nebraska. In making this submission, the City does not waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction. This notice may be supplemented with new information learned after submission.

On September 23, 2025, the City experienced a disruption to its computer network. As soon as the City became aware of the disruption, it took immediate action to secure its systems, which included taking networks offline, out of an abundance of caution. The City partnered with network specialists, to bring its networks back online and conduct an investigation into the nature and scope of the disruption. On or about September 28, 2025, the City determined that was taken from its network. The City commenced a thorough review of that data to understand what, if any, personal information was contained within the data set. The City concluded a portion of that review and notified potentially impacted current and former full, and part-time, employees/vendors. The data points potentially impacted for those individuals include the persons' names and Social Security numbers.

On November 19, 2025, the City provided written notice of the event to potentially impacted individuals, including one (1) Nebraska resident, via First Class U.S. mail. A sample copy of the notification letter is attached as Exhibit A.

Kennedys

The City's notice of this event included a brief description of the incident and encouragement to remain vigilant for incidents of fraud or misuse, from any source, by reviewing account statements and credit reports. The mailed notice also included the recommendation to file a report with law enforcement, notify their state attorney general, and/or contact the Federal Trade Commission for more information. The City confirmed the types of personal information subject to unauthorized access and shared the contact information for the major consumer reporting bureaus, state-specific regulators, and the number for a dedicated call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so. The City also offered the letter recipients twelve (12) months of credit monitoring and identity protection services through Kroll.

Upon learning of the event, the City took immediate action to secure its systems by taking networks offline. The City partnered with network specialists to bring its networks back online safely and securely and to thoroughly investigate. The City notified federal law enforcement. Additionally, the City is reviewing its existing security safeguards and policies already in place for ways to strengthen its systems to remain resilient against evolving threats. The City will also report to other state regulators as required.

This notice provides your Office with all information necessary to comply with Nebraska law. Please do not hesitate to contact me directly if you have additional questions.

Respectfully,

Nicholas S. Jajko

Nicholas Jajko
Partner
for Kennedys

Exhibit A

MICHIGAN CITY INDIANA

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<B2B_TEXT_2 (DBA ENTITY)>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

Re: ***Notice of Data Security Event***

Dear <<First_name>> <<Last_name>>:

The City of Michigan City, Indiana ("the City") writes to provide you with formal notice of the data security event that affected the City's computer networks. While we have no indications any information was subject to actual or attempted misuse, we take the privacy and security of your personal information seriously. We are providing you with these details of the event, our response, and resources you can take advantage of to help protect your personal information.

On September 23, 2025, the City experienced a disruption to our network. As soon as we became aware of the disruption, we took immediate action to secure our systems, which included taking our network offline, out of an abundance of caution. We partnered with network specialists, to bring our network back online and conduct an investigation into the nature and scope of the disruption. We notified federal law enforcement and our governing bodies. Additionally, we reviewed our existing security safeguards and policies already in place for ways to strengthen our systems to remain resilient against evolving threats.

On or about September 28, 2025, we determined that certain data was taken from our network. We then commenced a thorough review of that data to understand what, if any, personal information was contained within the data set. We concluded a portion of that review and are now notifying you and providing you with the enclosed resources out of an abundance of caution.

Our review of the data confirmed <<b2b_text_1 (impacted data elements)>> contained within certain files taken from our network. We reiterate that we have no indication of any actual or attempted fraud or misuse of your data. However, we are providing you with credit monitoring and identity protection services, as well as the enclosed resources, to take advantage of.

We secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Instructions for how to enroll in these services are below.

We encourage you to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider. Please refer to the enclosed "Steps You Can Take to Help Protect Your Information" for the additional resources you may take advantage of to protect against fraud and identity theft, should you find it appropriate to do so.

To activate and take advantage of the offered identity monitoring services, visit **https://enroll.krollmonitoring.com** to enroll.

*You have until **<<b2b_text_6 (activation deadline)>>** to activate your identity monitoring services.*

Kroll Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is enclosed.

If you have any questions or concerns, please contact our dedicated assistance line at (866) 613-1345, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your Kroll membership number ready when you call.

Please know that the City remains committed to protecting the information entrusted in its care.

Sincerely,

Angie Nelson Deuitch

Mayor Angie Nelson Deuitch
City of Michigan City

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Report Suspected Fraud. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.

Place Fraud Alerts. You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Place Security Freeze. As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com	**Experian** 1-888-397-3742 www.experian.com	**Equifax** 1-888-378-4329 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Obtain Additional Information. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; and www.marylandattorneygeneral.gov.

For New Mexico Residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/fair-credit-reporting-act/, www.ftc.gov, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

The City of Michigan City may be reached by mail at 100 E. Michigan Boulevard, Michigan City, IN 46360. This notice has not been delayed by law enforcement.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.